COMPUTER, TELECOMMUNICATIONS AND INFORMATION SECURITY 6441

(No.21 May 2016)

Responsibility

Division Chief
Camp Commander
Superintendent

The Camp Division Chief and Camp Commander/Superintendent shall develop a local procedure for computer security including; responsibilities of camp staff for assuring computer security, positive key control for any keys which unlock keyboards or CPU cases, storage of computer backup diskettes, and security requirements for each specific computer and computer work area.

All confidential employee information shall be secured and protected by both CDCR and CAL FIRE staff. Offenders that use computers are not allowed to access confidential employee information, including but not limited to, social security numbers, home addresses and home phone numbers.

All

CDCR and CAL FIRE staff members at conservation camps utilize computers during the course of their daily operations. State employees of CDCR or CAL FIRE are the only persons that may use a computer that has access to a modem. To maintain system security and minimize potential risks, the following procedures shall be followed when utilizing offenders to perform data entry:

1. An offender may not have a computer, modem, or terminal in his/her possession within the camp.
2. There shall be no offender access to a computer outside the offender's authorized work area.
3. Each computer shall be labeled to indicate whether offender access is authorized, and areas where offenders are authorized to work on computers shall be posted.
4. All computers within any offender's work area will be stand- alone units and shall only have authorized program and software files installed. Staff shall randomly access all offender computers to determine that only authorized programs are installed, and that computers are only being utilized for authorized work-related activity.
5. No offender may access any computer, under any circumstances, that is connected to a network, or have a modem installed. All such computers shall be password protected to preclude access.
6. No offender shall be permitted access to any computer unless the offender is under the direct supervision of a staff member and the computer is labeled "Authorized for Offender Access".

7. No offender will be permitted to use any computer designated as No Offender Access.
8. Under no circumstances will offenders, view, operate, or have access to any computer containing sensitive or confidential information.
9. Any computer containing documents with employee information such as addresses, telephone numbers, social security numbers, credit card numbers, driver's license numbers, or any other form of personal information shall be password protected to standards set by state policy. These computers must be designated either **"NO INMATE ACCESS" (DAI) or "NO WARD ACCESS" (DJJ)** computers.
10. Offenders shall not remove diskettes from authorized work areas. Possession of a diskette outside of the work area shall be deemed contraband and subject to disciplinary action.
11. Offenders shall not be permitted to possess any tool (such as screwdrivers, pliers, wrenches, files, etc.) while working on, or near any computer.

CAL FIRE - AGENCY SPECIFIC INFORMATION SECURITY 6441.1

(No.21 May 2016)

Responsibility

Division Chief

Each Camp Division Chief, under the guidance of the CAL FIRE Information Technology (IT) Coordinator shall be responsible for computer resources and information security within their operation at the camp. The Division Chief shall designate an information security coordinator for the camp who has the knowledge to supervise and ensure security measures are instituted. If no one in the camp has the knowledge of computer systems and database functions in this capacity, the Camp Division Chief must initiate a policy that prohibits offender use of any Departmental computer. In other words, if offenders know more about computers than the staff, they should not have access.

Any camp**,** which undergoes any change that causes the camp computer security not to meet the requirements of this policy, shall immediately inform CAL FIRE IT Coordinator. The IT Coordinator shall take immediate steps to remedy the security problem by whatever means are available.

TELECOMMUNICATION SECURITY 6441.2

(No.21 May 2016)

Responsibility

Division Chief
Camp Commander
Superintendent

The Camp Division Chief and Camp Commander shall develop a local procedure for the security of telecommunications systems (phones and faxes) at facilities where the offender clerks have been authorized in accordance with CCR Title 15 Section 3282(c) (DAI) to answer incoming business lines for the purpose of transferring telephone calls to staff within the facility and/or taking messages for staff if not available.

This procedure shall include a security plan that will include a section addressing fax machine access. Offenders are not authorized to operate fax machines.

ALL

All DAI offenders assigned as Clerks may be authorized to answer incoming business telephone calls for the purpose of taking messages or transferring calls to staff under the following guidelines:

1. DAI Offender Clerks per CDCR DOM Section 12070.6 shall answer all calls by stating “inmate (name).”
2. DAI Offender Clerks per CCR Title 15 Section 3282(c) (2) shall only answer a telephone capable of direct-dial connection with a public telephone system as authorized by staff.
3. Telephones normally used by DAI offender clerks shall not have dial-out capability.
4. Offender Clerks shall not use cellular or cordless phones.
5. All offenders authorized to answer incoming business telephone calls shall have a signed job description/duty statement and orientation that specifically authorized them to answer telephones and addresses the business use of telephones and faxes.

FORMS AND/OR FORMS SAMPLES: RETURN TO CAL FIRE LIBRARY HOME PAGE FOR FORMS/FORMS SAMPLES SITE LINK.

(see next section)

(see HB Table of Contents)